IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA v. LAFON ELLIS	Case No. 2:19-cr-00369-DWA

BRIEF OF ELECTRONIC FRONTIER FOUNDATION AND ACLU OF PENNSYLVANIA AS *AMICI CURIAE* IN SUPPORT OF DEFENDANT'S OPPOSITION TO GOVERNMENT'S MOTION TO QUASH

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

Constitutional Provisions

INTEREST OF THE *AMICI CURIAE*

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Pennsylvania is one of its affiliates. Transparency concerning algorithms used in criminal prosecutions is important to the work of a number of projects and programs at the ACLU, including the Racial Justice Program, the Speech, Privacy, and Technology Project, and the Criminal Law Reform Project. The ACLU and the ACLU of Pennsylvania have appeared in numerous cases, both as direct counsel and as amici, before courts in Pennsylvania and throughout the nation in cases involving the meaning and scope of the rights of criminal defendants and the legal limitations on the use of technology by police and prosecutors.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 30 years. With over 30,000 active donors, EFF represents the interests of people impacted by new technologies in court cases and broader policy debates surrounding the application of law in the digital age. EFF has special familiarity with and interest in constitutional issues that arise with new forensic technologies and has served as amicus in cases regarding a defendant's right to confront TrueAllele and other forensic software. E.g., *People v. Johnson*, No. F071640, 2019 WL 3025299 (Cal. Ct. App. July 11, 2019). EFF has also participated in the GAO's recent inquiry regarding forensic technology, including probabilistic genotyping, which was prompted by concerns from elected officials about the use of these technologies in criminal proceedings. *See Forensic Technology: Algorithms Used in Federal Law Enforcement, U.S.*

Government Accountability Office (May 12, 2020), https://www.gao.gov/products/GAO-20-479SP.[1]

POINTS AND AUTHORITIES

Is TrueAllele a widely-understood and vetted technology? Or does it function according to trade secrets in the source code that are, by definition, *secret*? Plainly, it cannot be both. In fact, it is probably neither, since it has not been subject to rigorous independent testing and may not contain anything that qualifies for trade secret protection at all.

The mere financial interests of a private party must not subjugate the fundamental rights of due process and confrontation enshrined in the Sixth and Fourteenth Amendments. A criminal defendant is entitled to an opportunity to review, analyze, and respond to the prosecution's evidence and simply cannot be required to blindly accept the claims of a vendor of forensic technology.

Independent review of source code, an essential and irreplaceable step in evaluating forensic software, routinely discovers errors in forensic tools. Such review of probabilistic genotyping technology of the same type as TrueAllele has previously exposed material mistakes—including ones unknown to their designers. No questioning of the designer or vetting of the abstract algorithm *intended* by the programmers can substitute for independent analysis or satisfy the constitutional protections that prevent injustice in criminal prosecutions.

Ostensibly, the secrecy of forensic software source code is meant to prevent commercial misappropriation, but it also prevents defendants and the public from discovering flaws in the software that sends innocent people to prison or execution. Time and again, independent review of forensic software has revealed errors and inconsistencies that call into question the technology's

[1] All Internet citations last visited July 23, 2020

viability and suitability for use in the criminal justice system. This includes counterparts to TrueAllele such as FST and STRMix, both of which have manifested serious errors that could cause them to inculpate innocent people.

Where the government seeks to use evidence generated by forensic software, disclosure of the software's source code is required by the Constitution's protections for criminal defendants and of the public's right to access court proceedings and see that justice is being done.

In the context of a criminal prosecution, where the public has a compelling interest in the Constitutional guarantees of a fair and public trial, public disclosure should be the rule. Only in very unusual circumstances – not present here – could the government establish such a weighty interest in secrecy that the public's right of access could be overridden. In such a case, the court could issue a protective order. Such orders are commonly used in commercial litigation between direct competitors, where the stakes are much lower and misappropriation likelier. It is never appropriate to deny the *defense* access to the source code and development materials or to deprive the accused of the ability to meaningfully confront the evidence against them.

Thus, the Court should deny the government's motion to quash.

I. Due Process and the Confrontation Clause Require Disclosure of Source Code Relied Upon by the Prosecution

U.S. criminal court proceedings are presumptively open to the public under both Supreme Court precedent and common law tradition. *See Richmond Newspapers, Inc. v. Virginia* 448 US 555, 580 n.17 (1980) (upholding presumption that criminal trials be open to public and recognizing common-law tradition "that historically both civil and criminal trials have been presumptively open."). Going even further, the Bill of Rights guarantees an accused the right to review and meaningfully confront the prosecution's evidence and prohibits the prosecution from shifting its burden of proof to the defense. U.S. Const. amend. VI, amend. XIV.

Accordingly, disclosure of evidence relied upon by the prosecution—even privately owned forensic software source code—is mandated by both our Constitution and common law.

A. Due Process Entitles Defense to Review the Prosecution's Evidence

Defendants have both a Constitutional and statutory right to receive and review the evidence against them. Evidence must be produced to the defense pursuant to both the Fourteenth Amendment guarantee of due process and the Sixth Amendment right to a fair trial. Recognizing the importance of ensuring the "fundamental fairness of trials," the Supreme Court has routinely ruled that material information otherwise protected by evidentiary privilege must be disclosed. *See, e.g.*, *Pennsylvania v. Ritchie*, 480 U.S. 39, 57 (1987) (disclosure of privileged conversations).

Moreover, Rule 16 of the Federal Rules of Criminal Procedure specifically requires that the government produce "documents, data," reports of "any scientific test or experiment," and expert evidence that the government intends to use at trial. FED. R. CRIM. P. 16(a)(1)(E), (F), (G).

The rights of the accused and the obligations of the government cannot be subjugated by the interest of private businesses in maintaining a purported trade secret and Mr. Ellis is entitled to review the source code upon which the prosecution's case relies.

B. Defense Review of Source Code Used by the Prosecution to Establish Guilt is Essential to the Right to Confrontation and a Fair Resolution of a Criminal Proceeding

Failure to disclose the source code violates Mr. Ellis's Sixth Amendment right to confront the evidence against him. The source code dictates the operation of an electronic program and is comprised of letters, numbers, symbols, and punctuation marks that often contain material errors as elementary as a misplaced ampersand.[2] The code can also reveal which—and precisely how—

[2] See Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 Cal. L. Rev. 179, 187 (2017); Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972, 1994 (2017) (quoting Sergey Bratus et al., *Software on the Witness Stand: What Should It Take for Us to Trust It?*, in Trust and Trustworthy Computing 396, 397 (Alessandro Acquisti et

assumptions are incorporated in the program and their effect on the outputted forensic evidence. The defense must be allowed to review the source code in order to understand and meaningfully confront the prosecution's key evidence of identity—an essential element of their case.

1. It is routine to discover software errors via adversarial and independent analysis

Software errors are extremely common. While some of these mistakes may be caught before products are released, many are not, costing the economy billions of dollars every year.[3] As software becomes ever more complex, and interacts with increasingly complicated systems, these bugs become harder to prevent.[4] Some are fairly easy to discover, such as one that causes a program to crash. But other errors are not as visible and the software will appear to function properly but output incorrect results. Such errors often go undiscovered for years.

The cause of these errors can be anything from creator biases coded into the program to misplaced punctuation. To take a famous and venerable example, the hole in the ozone layer went undiscovered for years because NASA's software was programmed to ignore outlier data that the original programmers had assumed was unrealistic.[5] A recent software error in Ireland's National Integrated Medical Imaging System "meant potentially thousands of patient records from MRIs,

---

al., eds., 2010)).

[3] *See* Michael Zhivich & Robert K. Cunningham, *The Real Cost of Software Errors*, *in* 7 IEEE Security & Privacy 87 (Mar. 1, 2009), https://ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2009_03_01_Zhivich_IEEES-P_FP.pdf

[4] Roger A. Grimes, *Five Reasons Why Software Bugs Still Plague Us,* CSO Online (July 8, 2014), https://www.csoonline.com/article/2608330/security/5-reasons-why-software-bugs-still-plague-us.html.

[5] Michael King and David Herring, *Research Satellites for Atmospheric Sciences, 1978-Present, Serendipity and Stratospheric Ozone*, NASA's Earth Observatory (Dec. 10, 2001), https://earthobservatory.nasa.gov/Features/RemoteSensingAtmosphere/remote_sensing5.php.

X-rays, CT scans and ultrasounds were recorded incorrectly."[6] The error involved a misplaced less-than (<) symbol and may have led to thousands of unnecessary medical procedures. A large Australian bank recently admitted a software error had caused it to fail to report certain transactions for almost three years, leading to widespread money laundering.[7] In rare cases, software errors may even be intentional, as was the case with Volkswagen software designed to make its vehicles produce inaccurate emissions readings during testing.[8] Of course, the vast majority of software errors are merely oversights, but that does not lessen the seriousness of their impact.

Most of these errors would not have been discoverable by merely questioning the program's creators or users. Just like all other complex software, modern forensic technology, such as the new generation of DNA tools, is at risk of error.[9] Independent public scrutiny and testing is the best—and often only—way to discover such errors.[10]

2. Probabilistic DNA tools embody a variety of potentially flawed assumptions and warrant rigorous independent examination and testing

In 2017, the President's Council of Advisors on Science and Technology (PCAST) issued a report emphasizing the need for independent review of probabilistic DNA programs, in part, to

---

[6] Jack Power, *Software company behind HSE scan glitch begins investigation*, The Irish Times (Aug. 5, 2017), https://www.irishtimes.com/news/ireland/irish-news/software-company-behind-hse-scan-glitch-begins-investigation-1.3178349.

[7] Allie Coyne*, CBA blames coding error for alleged money laundering*, itnews (Aug. 7, 2017), https://www.itnews.com.au/news/cba-blames-coding-error-for-alleged-money-laundering-470233.

[8] Sonari Glinton, *How A Little Lab In West Virginia Caught Volkswagen's Big Cheat*, NPR Morning Edition (Sept. 24, 2015), http://www.npr.org/2015/09/24/443053672/how-a-little-lab-in-west-virginia-caught-volkswagens-big-cheat.

[9] Roth, *supra*; Chessman, *supra*.

[10] Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques*, 66 DePaul L. Rev. 97 (Fall 2016) .

determine "whether the software correctly implements the methods" on which the analysis is based.[11] The necessity of independent source code review was starkly demonstrated when FST (a counterpart to TrueAllele used in New York crime labs) was finally provided to a defense team for analysis. The defense expert discovered a previously undisclosed portion of the code that could incorrectly tip the scales in favor of the prosecution's hypothesis that a defendant's DNA was present in a mixture. Reply Memorandum of Law in Support as to Kevin Johnson at 17-19, *United States v. Kevin Johnson*, (S.D.N.Y. Feb. 27 2017) (No. 15-CR-565 (VEC), D.I. 110). They also determined that the code actually used in the crime labs differed from the code of the seemingly same program used to validate the results. *Id*.

Likewise, when STRMix (another probabilistic DNA tool similar to TrueAllele) was analyzed by independent researchers, they found programming errors that created false results in 60 cases in Queensland, Australia.[12]

The problems caused by nondisclosure are especially acute in the context of the latest generation of probabilistic DNA analysis because there is no objective baseline truth against which the output from the program may be evaluated. The importance of a baseline is demonstrated in the breathalyzer context. It is possible to determine, as an objective fact, the parts per million of alcohol in the air using existing non-portable technology. Thus, emerging portable devices can be evaluated by comparing their results with the factual measurement. Even so, courts nonetheless

---

[11] President's Council of Advisors on Science and Technology (PCAST), *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* 78 (Sept. 2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[12] David Murray, *Queensland authorities confirm 'miscode' affects DNA evidence in criminal cases*, Courier Mail (Mar. 20, 2015), http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b

require independent review of the code that runs breathalyzers. *State v. Chun*, 194 N.J. 54, 127 (2008) (error in one version of breathalyzer code resulted in incorrect results); *see State v. Underdahl*, 767 N.W.2d 677 (Minn. 2009) (potential defects that could be detected in breathalyzer source code warranted order to disclose complete source code); *see also Davenport v. State* 289 Ga. 399, 404 (2011) (Nahmias, J., *concurring*) (noting potential due process concerns if source code for forensic machines could not be discovered, lauding majority decision for rejecting such a conclusion and remanding).

The latest generation of DNA analysis tools cannot be measured against an objective truth. Unlike in the context of breathalyzers, these programs are not designed to output an objectively measurable value, as evident from the fact that different programs and even different laboratories using the same program will generate substantially different results for the same sample. Each analysis is specific to the sample that was tested, such as a swab from a weapon, which are often mixtures of DNA from multiple sources, as is alleged in Mr. Ellis's case. *See People v. Collins*, 49 Misc.3d 595, 613-616 (Kings Co. Sup. Ct. 2015).

Furthermore, the analysis of the sample is dictated by the particular assumptions programmed into the device.[13] This creates the incredibly worrisome result that different software, like STRMix and TrueAllele, provide drastically different probability calculations from one another—a discrepancy that can mean the difference between exculpation and inculpation.[14] *See*

---

[13] *See*, *e.g.*, Paolo Garofano, et. al., *An Alternative Application of the Consensus Method to DNA Typing Interpretation for Low Template-DNA Mixtures*, Forensic Sci. Int'l: Genetics Supp. Series 5, e422–e424 (2015).

[14] PCAST, *supra*, 79 n.212. *See, e.g.*, *People v. Hillary,* Court No. 2015-15 (N.Y. Sup.Ct. St. Lawrence Co. 2016), http://www.northcountrypublicradio.org/assets/files/08-26-16DecisionandOrder-DNAAnalysisAdmissibility.pdf. *See* Jesse McKinley, *Oral Nicholas Hillary Acquitted in Potsdam Boy's Killing,* N.Y. Times (Sept. 28, 2016), http://www.nytimes.com/2016/09/29/nyregion/oral-nicholas-hillary-potsdam-murder-trial-garrett-phillips.html. *See also* PCAST, *An Addendum to the PCAST Report*, 8,

Commonwealth v. Foley, 38 A.3d 882, 887, 890 (Pa. Super. Ct. 2012) (noting that TrueAllele calculated a match statistic of 189 billion, compared to a competitor's estimate of 13,000—a more than 14-million-fold difference). Consequently, these programmed assumptions, and the way they are coded into the software, are critical to the defense's ability to identify areas for challenges to its reliability and accuracy.

Other common random effects can also alter DNA test results, and DNA analysis tools take different approaches to counteracting these effects or may ignore them altogether. *See Collins,* 49 Misc.3d at 600, 604-606 (discussing stochastic effects in context of analyzing admissibility of probabilistic genotyping program). Two of these random phenomena are "allelic drop-in" and "allelic drop-out," which simply refer to the rate at which the technology ignores alleles (DNA patterns) or falsely reports their presence in a mixture. *Id*. at 605-606. The other common phenomena are more complicated, referred to as "exaggerated stutter" and "peak height imbalance," and these create the appearance of alleles that are in fact absent, or inaccurately make it seem that an allele is far more prevalent than others. *Id.* at 606-610.

The only method of ascertaining precisely how these effects are accounted for, if at all, is to examine the source code.

3. The Confrontation Clause entitles the defense to review the prosecution's evidence

Given the foregoing, meaningful confrontation of the TrueAllele program test results necessarily depends on the defense's access to and opportunity to review the source code and the assumptions embedded within it. A fair trial necessitates that the accused to "be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; [and] to have

---

https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensics_addendum_finalv2.pdf; Garofano, *supra*, at e422–e424.

compulsory process for obtaining witnesses in his favor." U.S. Const. amend. VI. The right to confrontation is procedural and cannot be disposed of simply because the evidence appears reliable. *Crawford v. Washington,* 541 U.S. 36, 62 (2004) ("Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty.").

The Confrontation Clause's animating concern is "to ensure the reliability of the evidence . . . by subjecting it to rigorous testing." *Maryland v. Craig*, 497 U.S. 836, 845 (1990). The Supreme Court has recognized that this concern applies with full force to forensic evidence. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 313 (2009) (holding that affidavits reporting the results of a forensic analysis of seized drugs are testimonial and subject to the Confrontation Clause); *Bullcoming v. New Mexico*, 564 U.S. 647, 663–64, 666 (2011) (holding that certification on a forensic laboratory report is testimonial and defendant has a right to confront the specific analyst who made the certification).

In the modern context, black-box technologies like TrueAllele squarely parallels the *ex parte* examinations that motivated the founders to adopt the Confrontation Clause in the first place. Performed at the government's demand, intentionally opaque in its operation, and unduly impressive to the jury, both render the defendant powerless to test the credibility of the source and undermine the state's case against him. One side (the prosecution) would have use of evidence reasonably believed to be essential to a fair resolution of the lawsuit—namely, the program methodology that must be examined for accuracy, functionality and credibility in order to meaningfully confront the test results—which was denied to the opposing party. Thus, disclosure is necessary to ensure that Mr. Ellis receives a "fair trial, understood as a trial resulting in a verdict worthy of confidence." *Kyles v. Whitley*, 514 U.S. 419, 434 (1995).

4. Exclusion of the DNA evidence is the appropriate remedy for non-disclosure

Where the prosecution refuses to disclose evidence upon which it relies, exclusion is the only appropriate remedy. Our justice system cannot permit convictions based on secret evidence. *See* U.S. Const. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial…and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor,"); *Richmond Newspapers*, 448 U.S. at 580 (First amendment requires criminal trials be open to the public). To do so would pervert the equitable principles upon which our common law right to access criminal proceedings and our Constitutional guarantee of due process were founded. *Id*. at 580, n.17 (recognizing the common-law tradition "that historically both civil and criminal trials have been presumptively open."); U.S. Const. amend. XIV.

C. Due Process Prohibits Burden Shifting to the Defense

The Fourteenth Amendment safeguards individual rights to due process of law, which dictate that "a State must prove every ingredient of an offense beyond a reasonable doubt, and . . . may not shift the burden of proof to the defendant . . . ." *Patterson v. New York*, 432 U.S. 197, 215 (1977). By the same token, "a presumption which, although not conclusive, had the effect of shifting the burden of persuasion to the defendant," is unconstitutional. *Sandstrom v. Montana*, 442 U.S. 510, 524 (1979); *see generally*, *Mullaney v. Wilbur* 421 U.S. 684 (1975). Thus, any framework that imposes an evidentiary burden upon defense as a prerequisite to obtaining access to evidence that forms the basis of the criminal prosecution both contorts and contravenes basic Constitutional guarantees and cannot withstand scrutiny.

The prosecution may not shift the burden of persuasion to the defense to show that the evidence that forms the backbone of the prosecution's forensic case is relevant to the defense

theory, especially without having the opportunity to examine the evidence in the first place. It's akin to asking a mechanic to certify a car as in good working condition without allowing them to look under the hood. There are many things that could affect or influence the car's drivability, but they won't know until they inspect it. Because this framework fails to protect basic Constitutional guarantees, this Court should firmly reject it.

II. Requiring Disclosure Is Necessary to Protect the Public's First Amendment Right of Access to Courts

Denying the government's motion to quash the subpoena will ensure that the public's qualified First Amendment right of access will attach to any materials about TrueAllele that are entered into the record or become the subject of substantive litigation. Such materials may range from the algorithm's source code to Cybergenetics' internal validation studies to any eventual defense expert reports.

Once the right of access attaches, proceedings and records are presumptively open to the public, but they may be closed where there are "specific, on the record findings" that "closure is essential to preserve higher values and is narrowly tailored to serve that interest." *Press-Enter. Co. v. Superior Court ("Press-Enter. II")*, 478 U.S. 1, 13, 14–15 (1986) (quoting *Press-Enter. Co. v. Superior Court* ("*Press-Enter. I*"), 464 U.S. 501, 510 (1984)); *see also Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 606–07 (1982); *N.Y. Civil Liberties Union v. N.Y.C. Transit Auth.*, 684 F.3d 286, 296 (2d Cir. 2012) (requiring a substantial probability of harm to a compelling government interest, and no alternative that can effectively protect against that harm to overcome presumption of access).

A. The First Amendment Right of Access Exists to Allow the Public to Meaningfully Oversee Courtroom Proceedings

The First Amendment guarantees "the right to attend criminal trials" and to "'receive information and ideas.'" *Richmond Newspapers*, 448 U.S. at 556, 576 (quoting *Kleindienst v. Mandel*, 408 U.S. 753, 762 (1972)).

Public access to materials about TrueAllele will ensure that widespread problems—whether in the algorithm's design, the source code that is intended to implement it, or the algorithm owner's approach to delivering results—can be efficiently audited by independent experts. Allowing the public, including academics and other experts, to examine such evidence would markedly improve the reliability and fairness of such evidence in criminal trials.

This would achieve one of the main purposes of the First Amendment right of access, which attaches to criminal trials to allow the public to observe and evaluate the workings of the criminal justice system—and to make changes in order to eliminate injustice. *See id.* at 572. As the Supreme Court has explained, "the criminal justice system exists in a larger context of a government ultimately of the people, who wish to be informed about happenings in the criminal justice system, and, if sufficiently informed about those happenings, might wish to make changes in the system." *Gentile v. State Bar of Nev.*, 501 U.S. 1030, 1070 (1991). The need for public oversight of government process is strongest in criminal trials, where the state wields its greatest power to affect individual liberty. Public access "enhances the quality and safeguards the integrity" of the judicial process, "heighten[s] public respect" for that process, and "permits the public to participate in and serve as a check upon the judicial process." *Globe Newspaper*, 457 U.S. at 606.15

---

[15] The importance of public access to criminal trials is also embedded in the common law, *see, e.g., Lugosch v. Pyramid Co.*, 435 F.3d 110, 119 (2d Cir. 2006), as well as the Sixth Amendment, which guarantees a criminal defendant the right to a public trial. *See, e.g., In re Oliver*, 333 U.S. 257, 267–68 (1948). Indeed, the Supreme Court has suggested that the demands of the Sixth's Amendment's public-trial right—grounded in the defendant's right to a fair trial—

Under the Supreme Court's prevailing "experience and logic" test, the public's First Amendment right of access attaches to judicial proceedings and records where (a) the type of judicial process or record sought has historically been available to the public, and (b) the public access plays a "significant positive role" in the functioning of the process itself. *Press-Enter. II*, 478 U.S. at 9, 11; *see Globe Newspaper*, 457 U.S. at 605–07.

B. The Broad Reach of the First Amendment Right of Access Encompasses Software Used to Produce Evidence Introduced to Prove the Guilt of a Defendant

Assuming that this case will proceed to trial, there is little question that the right of access will attach. Indeed, the Supreme Court grounded the First Amendment "presumption of openness [that] inheres in the very nature of a criminal trial under our system of justice" in the "unbroken, uncontradicted history" of such access, "supported by reasons as valid today as in centuries past." *Richmond Newspapers*, 448 U.S. at 573; *see also Press-Enter. I*, 464 U.S. at 505–08 (discussing history of openness in criminal trials); *Cal. First Amendment Coal. v. Woodford*, 299 F.3d 868, 874 (9th Cir. 2002); *KNSD Channels 7/39 v. Superior Court*, 74 Cal. Rptr. 2d 595, 596–97 (Cal. Ct. App. 1998).

And once the right attaches to a proceeding, the presumption of access applies broadly to all materials essential to that proceeding—including the algorithmic source code in this case. *See Doe v. Pub. Citizen*, 749 F.3d 246, 267 (4th Cir. 2014) ("[T]he First Amendment right of access extends to materials submitted in conjunction with judicial proceedings that themselves would trigger the right to access."); *see also In re Application of WFMJ Broad. Co.*, 566 F. Supp. 1036,

---

may go even further than the First Amendment right in certain cases. *See Presley v. Georgia*, 558 U.S. 209, 213 (2010); *Waller v. Georgia*, 467 U.S. 39, 46 (1984) ("There can be little doubt that the explicit Sixth Amendment right of the accused is no less protective of a public trial than the implicit First Amendment right of the press and public.").

1040 (N.D. Ohio 1983) ("Just as the Supreme Court's reluctance to embrace a 'narrow, literal conception of the [First] Amendment's terms', *Globe Newspaper* [, 457 U.S. at 604], gave rise to a constitutional right of access to criminal trials, the same view could make a constitutional right to evidence an appropriate adjunct to insure that such proceedings are 'open.'").

As the Ninth Circuit recognized in *Woodford*, meaningful access to a proceeding means access to its nuts and bolts. In *Woodford*, a lethal injection case, that meant a right to view "executions from the moment the condemned is escorted into the execution chamber." 299 F.3d at 870–871, 877. The court explained that, for the right of access to accomplish its goals, "citizens must have reliable information about the 'initial procedures,' which are invasive, possibly painful and may give rise to serious complications." *Id.* at 876–77. The same must be true for algorithms that produce the prosecution's material evidence in a criminal trial—which also have the potential for serious complications and inaccuracies. Just as without access to the initial procedures of an execution, "the public will be forced to rely on the same prison officials who are responsible for administering the execution to disclose and provide information about any difficulties with the procedure," without access to the algorithms that create material evidence, the public will be forced to rely on the same government officials responsible for introducing the evidence and convincing the judge and jurors that they should trust it – or the vendors who profit from selling the technology and related services. *Id*. at 883. And much like prison officials, these persons "do not have the same incentives to describe fully the potential shortcomings of" their evidence. *Id*. at 884. Here, as in *Woodford*, the government cannot artificially cabin the record of a proceeding in order to deny public access to all but the ultimate result.[16]

[16] Courts have held that the public's First Amendment right of access attaches to materials in the record of a criminal case for this reason. *See, e.g.*, *In re Globe Newspaper Co.*, 729 F.2d 47 (1st Cir. 1984) (right of access attaches to memorandum, affidavits and transcripts in criminal case); *In*

Moreover, the work of one legal scholar suggests that limiting access on the basis of a purported trade secret privilege would be ahistorical. Rebecca Wexler has found that "[e]arly historical sources suggest that the [trade secrets] privilege"—precisely the tool companies are now using to keep algorithms out of the record of criminal cases—was historically "unavailable in criminal proceedings." Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stan. L. Rev. 1343, 1388–90 (2018). Rather, historically, courts have ordered trade secrets be disclosed, even when there were requests for nondisclosure. *See id*. (discussing *The King v. Maha Rajah Nundocomar*, 20 Howell State Trials 923, 1057 (1775), and *R v. Webb*, 174 Eng. Rep. 140 (1834)).

This suggests that permitting the State to keep source code hidden on the basis of a trade secret privilege would block from view information of a type that would historically have been public. Similarly, an attempt to shield material from disclosure on the assertion of a copyright would contradict precedent allowing for distribution and copying in the context of litigation. *See, e.g., Bond v. Blum*, 317 F.3d 385, 396 (4th Cir. 2003) (abrogated by *Kirtsaeng v. John Wiley & Sons, Inc.*, 136 S. Ct. 1979 (2016), on other grounds) (recognizing that "the societal benefit of having all relevant information," including copyrighted materials, "presented in a judicial proceeding is an important one").

Moreover, there is immense public value in openness with forensic algorithms. There is a long history of junk science employed under the guise of technological advancement in criminal cases—and of public access to and analysis of such evidence as the means to its eventual

---

re N.Y. Times Co., 828 F.2d 110 (2d Cir. 1987) (same for suppression motions and exhibits); *In re Wash. Post Co*., 807 F.2d 383 (4th Cir. 1986) (same for plea agreements); *United States v. Peters*, 754 F.2d 753, 763 (7th Cir. 1985) (same for trial exhibits).

invalidation. "Since a series of high-profile legal challenges in the 1990s increased scrutiny of forensic evidence, a range of long-standing crime-lab methods have been deflated or outright debunked," including bite-mark analysis, ballistics testing, fingerprinting, and microscopic-hair-comparison. Matthew Shaer, *The False Promise of DNA Testing*, Atlantic (June 2016), http://theatln.tc/2xs7XUL.

Indeed, the Supreme Court has relied on public scrutiny of forensic processes to inform its interpretation of constitutional protections. *See Melendez-Diaz*, 557 U.S. at 319 ("Serious deficiencies have been found in the forensic evidence used in criminal trials."). And state supreme courts—as well as federal appellate courts—have equally looked to work done by the public, rather than either party or its experts in a criminal case, to determine that evidence based on specific technologies was not sufficiently reliable to be admissible into evidence. *See, e.g., Han Tak Lee v. Houtzdale SCI*, 798 F.3d 159, 166–67 (3d Cir. 2015) (discussing changes in "fire–science"); *People v. Leone*, 21155 N.E.2d 696 (N.Y. 1969) (relying on commentary of outside experts to hold that evidence derived from polygraph tests was not fit for admission); *see People v. Davis*, 72 N.W.2d 269, 281– 82 (Mich. 1965) (same).

Public scrutiny has had substantial benefits outside of the courtroom as well, leading to important improvements in investigative fields. For example, after a *New Yorker* article exposed a flawed case based on fire-science evidence, Texas not only "reconsider[ed] old cases that had been improperly handled by the original investigators," but also "reinvented itself as a leader in arson science and investigation" by "revamp[ing] the state's training and investigative standards." Jeremy Stahl, *The Trials of Ed Graf*, Slate (Aug. 16, 2015), https://perma.cc/89TJ-4ASK.

And all of this is true of the previous generation of DNA evidence as well. In this field "[b]oth the initial recognition of serious problems and the subsequent development of reliable

procedures were aided by the existence of a robust community of molecular biologists" and by "judges who recognized that this powerful forensic method should only be admitted as courtroom evidence once its reliability was properly established." PCAST, *supra*, at 26.

Public access would plainly enhance the reliability of algorithmic evidence, especially software like probabilistic genotyping software that have been minimally tested in the field. Most existing validation studies of probabilistic DNA typing have been "conducted under idealized conditions unrepresentative of the challenges of real casework." Roth, *supra*; see also Christopher D. Steele & David J. Balding, *Statistical Evaluation of Forensic DNA Profile Evidence*, 1 Ann. Rev. Stat. & App. 361, 380 (2014). While TrueAllele "appear[s] to be reliable for three-person mixtures in which the minor contributor constitutes at least 20 percent of the intact DNA in the mixture and in which the DNA amount exceeds the minimum level required for the method," "there is relatively little published evidence" for "more complex mixtures"—that is, precisely the sort of mixtures for which these programs are used in actual cases – including this one. PCAST, *supra*, at 80-81. Moreover, "most of the studies evaluating software packages have been undertaken by the software developers themselves." *Id*. at 80. Public access to algorithmic evidence would improve the role such evidence plays in criminal trials—including by preventing the jury from giving it undue weight, where necessary—and increase the public's confidence in the justice system more generally.[17]

[17] The government may argue that requiring the release of source code will have a negative effect on the proceedings because it will create additional disputes, but that argument would be misplaced. The government has no valid interest in saving time by conducting unfair proceedings. Moreover, public vetting of algorithmic source code will surely experience efficiency gains as it becomes a more commonplace check on complex, experimental evidence. As the Supreme Court recently reaffirmed, "the Government's 'interest . . . in a criminal prosecution is not that it shall win a case, but that justice shall be done.'" *Turner v. United States*, 137 S. Ct. 1885, 1893 (2017) (quoting *Berger v. United States*, 295 U.S. 78, 88 (1935)).

As one scholar, Erin Murphy, has explained, numerous factors that plague the defense in criminal trials—including "structural asymmetry[,] . . . scarcity of resources, weak discovery practices, and high rate of plea bargaining"—make the "adversarial process an inadequate safeguard of the integrity of forensic science." Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 Calif. L. Rev. 721, 757 (2007). But experts reviewing publicly disclosed information about algorithms, including the source code, should be free of these obstacles and should have the time, resources, and expertise to effectively and efficiently audit the algorithmic programs. Independent review of documents across cases may catch errors or mistakes that would not be identifiable in one case alone. Murphy, *supra*, at 773.

In a 2008 case, a defense expert's review of Alcotest 7110 source code in one case—which "documented 19,500 errors, nine of which he believed could ultimately affect the breath alcohol reading," Roth, *supra*, at 1995 (internal marks omitted)—led the New Jersey Supreme Court in another case to require modifications to prevent misleadingly high accuracy readings. *Chun,* 943 A.2d at 120–21. And, the errors with FST were only discovered after independent source code review.[18] In other words, such secrecy hurts the criminal justice system on all sides, impeding the process not only for the defense but for the prosecution as well. The expert reports submitted in that case are now publicly available and FST's source code is on GitHub.[19]

---

[18] After the independent review of the FST code, New York recognized that the secrecy surrounding FST had "exacerbated the substantial misunderstanding of fundamental aspects of the FST source code." Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, ProPublica (Oct. 20, 2017, 8:00 A.M.), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence.

[19] *See New York City's Forensic Statistical Tool*, GitHub, https://perma.cc/348Z-6W6M (last updated Oct. 20, 2017)

And though some courts have (erroneously) applied a narrower test to determining whether the First Amendment right-of-access attaches—looking to the nature of a particular document rather than proceedings themselves, *see In re Bos. Herald, Inc.*, 321 F.3d 174, 182–84 (1st Cir. 2003) (reviewing case law applying the First Amendment right of access to proceedings and documents)—the right would still attach to information about an algorithm used to produce evidence of guilt in a criminal case under this analysis. Under the test's "experience" prong, it is not only well established but fundamental that the materials essential to the government's case in chief enjoy a presumption of openness in the criminal justice system. *See, e.g., In re Application of WFMJ Broad. Co.*, 566 F. Supp. at 1040 (tapes played to jury in open court); *United States v. Posner*, 594 F. Supp. 930, 934–35 (S.D. Fla. 1984) (tax returns admitted into evidence); *United States v. Scott*, 48 M.J. 663 (A. Ct. Crim. App. 1998) (materials entered into evidence at trial); *Valley Broad. Co. v. U.S. Dist. Court*, 798 F.2d 1289, 1292–93 (9th Cir. 1986) (transcripts of exhibits); *In re Times-World Corp.*, 488 S.E.2d 677 (Va. 1997) (documents submitted into evidence). And the right also attaches to supporting materials that form a critical component of the record, especially when they pertain to the "adjudicat[ion of] substantive rights," *Rushford v. New Yorker Mag.*, 846 F.2d 249, 252 (4th Cir. 1988).[20]

[20] Moreover, the "experience" prong "is not meant . . . to be construed so narrowly" as to exclude from First Amendment coverage proceedings or documents that are of "relatively recent vintage." *In re Bos. Herald*, 321 F.3d at 184. In such cases, courts look to analogous proceedings and documents of the same "type or kind." *Rivera-Puig v. Garcia-Rosario*, 983 F.2d 311, 323 (1st Cir. 1992) (emphasis omitted); *see El Vocero de P.R. v. Puerto Rico*, 508 U.S. 147, 150–51 (1993) (finding pretrial criminal hearings in Puerto Rico analogous to other pretrial hearings to which First Amendment right applies, despite distinctions noted by Puerto Rico Supreme Court); *Press–Enter. II*, 478 U.S. at 10–11 (evaluating California pre-trial hearings by looking to practices of other states and to other types of hearings, including probable cause hearing in Aaron Burr's 1807 trial for treason); *see also United States v. Chagra*, 701 F.2d 354, 363 (5th Cir. 1983) ("Because the first amendment must be interpreted in the context of current values and conditions, the lack of an historic tradition of open bail reduction hearings does not bar our recognizing a right of access to such hearings." (citations omitted)).

While courts have held that the "raw fruits" of discovery may not be subject to the right of access, *see, e.g., id.; Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984)*, that conclusion is altered where the parties rely on or incorporate discovery materials into substantive litigation. Indeed, in the civil context courts have held that under the First Amendment, reports relied upon by parties in the "adjudication stages" of litigation are presumptively "available for public inspection unless exceptional circumstances require confidentiality." *In re Continental Ill. Sec. Litig.*, 732 F.2d 1302, 1314 (7th Cir. 1984); *accord Joy v. North*, 692 F.2d 880, 893 (2d Cir. 1982); *see also Rushford*, 846 F.2d at 253 (documents filed in connection with summary judgment motion); *NBC Subsidiary (KNBC-TV), Inc. v. Superior Court*, 980 P.3d 337, 360 n.28 (Cal 1999) (applying the same principle in a civil context).[21] Those principles apply with even greater force in the criminal context to evidence and its attendant documents, *see, e.g., In re Wash. Post Co.*, 807 F.2d at 389–90 — and, assuming this case proceeds to trial or any proceeding or briefing that adjudicates substantive rights, this would encompass information about an algorithm that produces the evidentiary results at the center of the government's case. *See Doe*, 749 F.3d at 267.

As discussed above, the "logic" prong also dictates that the First Amendment right of access attaches in this context. Public access to the highly complex algorithmic source code that produced the evidence that will be used against Mr. Ellis at trial would "enhance[] the quality and safeguard[] the integrity of the factfinding process, with benefits to both the defendant and to society as a whole," *Globe Newspaper Co.*, 457 U.S. at 606; *see also, e.g., Grove Fresh Distribs.,*

[21] Even courts that have rejected the attachment of a First Amendment right of access in particular contexts have acknowledged that the right may well attach where "the material is important and the decision to which it is relevant amounts to an adjudication of an important substantive right." *Anderson v. Cryovac, Inc.*, 805 F.2d 1, 11 (1st Cir. 1986).

Inc. v. Everfresh Juice Co., 24 F.3d 893, 897 (7th Cir. 1994) (citing *Richmond Newspapers*, 448 U.S. at 555).[22]

Public access to the foundation of the algorithmic evidence introduced against Mr. Ellis will allow for a thorough public vetting of a new technology, with all its salutary consequences. In particular, in the context of criminal cases in which defendants and their counsel have limited resources, public access to algorithmic evidence would bolster courts' ability to "ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable," *Daubert v. Merrell Dow Pharm., Inc*., 509 U.S. 579, 589 (1993), by providing the public with an opportunity to evaluate and test evidentiary material.[23]

III. The Defense Has a Complete Right to the Information

If a case did present extraordinary circumstances that justified withholding the operation of a forensic technology from the public, the proper course would be for the court to issue a

[22] *See also Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 998 F.2d 157, 161 (3d Cir. 1993) ("As with other branches of government, the bright light cast upon the judicial process by public observation diminishes the possibilities for injustice, incompetence, perjury, and fraud. Furthermore, the very openness of the process should provide the public with a more complete understanding of the judicial system and a better perception of its fairness." (quoting *Rep. of Phil. v. Westinghouse Elec. Corp.*, 949 F.2d 653, 660 (3d Cir. 1991)); *United States v. Hubbard*, 650 F.2d 293, 315 n.79 (D.C. Cir. 1980) (Like the public trial guarantee of the Sixth Amendment, the First Amendment right of access serves to "safeguard against any attempt to employ our courts as instruments of persecution," to promote the search for truth, and to assure "confidence in . . . judicial remedies.").

[23] To be clear, a *Daubert* hearing is plainly an insufficient substitute for scrutiny of algorithmic source code, as it goes only towards admissibility (a matter decided by the judge), rather than weight (a matter decided by the jury). *See Amorgianos v. National R.R. Passenger Corp*., 303 F.3d 256, 266-67 (2d Cir. 2002) (distinguishing a factor affecting weight from factors to be considered under *Daubert*'s admissibility standard). Any flaws or errors in source code would tend to undermine the value of state evidence based on it and would permit the defendant to argue to the jury to disregard the experimental test results introduced into evidence.

protective order guaranteeing the defense had access to the information—or else to exclude the fruits of that technology from the case.

A. The Source Code May Not Be Withheld from Defense Attorneys and Experts

As a general rule, the prosecution is obligated to disclose evidence and the only exception for withholding is if the material is the prosecution's work product or certain statements by prospective government witnesses in the case. FED. R. CRIM. P. 16(a)(2) ("Information not subject to disclosure"). Outside of those narrow exceptions, no relevant evidence, even if privileged, is automatically protected from disclosure. *See, e.g., Ritchie*, 480 U.S. at 57.

Where the prosecution claims a trade secret privilege, it or the trade secret owner must first carry the burden of showing "good cause." FED. R. CRIM. P. 16(d)(1); *see* 18 U.S.C. § 1835(b) (rights of trade secret owners). Even when that burden is met, disclosure to the defense is nevertheless required, but the court may impose a protective order. *See* FED. R. CRIM. P. 16(d).

As demonstrated by their widespread use in civil litigation—where there is no liberty interest at stake and the parties are likely to be market competitors—protective orders are more than sufficient to ensure the interests of trade secret holders. In those cases, the orders allow attorneys and experts representing the competitors to view the evidence but may withhold access from others. Employment of these orders are so ubiquitous, in fact, that many federal district courts have adopted model protective orders for patent litigation that specifically contemplate the disclosure of trade secrets and source code to counsel and experts retained by an opposing party who agree to comply with the order.[24] Protective orders, rather than blanket denial of disclosure

[24] *See, e.g.*, *Local Patent Rules*, U.S. District Court for the Western District of Pennsylvania, Appendix LPR 2.2, http://www.pawd.uscourts.gov/sites/pawd/files/Local%20Patent%20R%20-%2012-5-2015.pdf ; *Model Protective Orders*, United States District Court, Northern District of California, http://www.cand.uscourts.gov/model-protective-orders. In litigation between competitors concerning actual trade secret source code, extreme precautions are sometimes

requests, are used even when the parties are direct competitors with an interest in profiting from proprietary information of the other.[25]

Consequently, the information must be disclosed to the defense.

B. Any Protective Order Restricts the Public's Right of Access and Must Be Narrowly Tailored to Comport With the First Amendment.

Because the right of access is a qualified one, the outcome, in this case or any other, will depend upon the strength of the government's interest in continued secrecy, as well any measures taken to narrowly tailor the denial of the source code to the public, including through a protective order. *See Press-Enter. II*, 478 U.S. at 13–14; *see also Globe Newspaper Co.*, 457 U.S. at 608 (explaining that even a compelling government interest "does not justify a *mandatory* closure rule, for it is clear that the circumstances of the particular case may affect the significance of the interest"); *United States v. Amodeo*, 71 F.3d 1044, 1049 (1995); *Grove Fresh Distribs.*, 24 F.3d at 898. And that process will require the government, and then the court, to make on-the-record findings concerning the reasons justifying full or partial secrecy. *See Press-Enter. II*, 478 U.S. at 13–14.

It is clear, however, that where a criminal case involves algorithmic source code that produces material evidence like that in Mr. Ellis's case, the strength of the public's right of access should favor some level of disclosure. Indeed, the Supreme Court has explained that the "circumstances" in which "the right to an open trial may give way . . . to other rights or interests . . . will be rare." *Waller*, 467 U.S. at 45. Such sufficiently weighty rights and interests might include, for example, "the defendant's right to a fair trial or the government's interest in inhibiting

---

necessary, but even there it is improper to withhold the evidence.

[25] Dustin B. Benham, *Proportionality, Pretrial Confidentiality, and Discovery Sharing* 71 Wash. & Lee L. Rev. 2181, 2240-41 (2014).

disclosure of sensitive information." *Id.* But the government's interest in this case and those like it does not approach that class of gravity. To the contrary, the defendant's right to a fair trial dovetails—rather than conflicts—with the public's right of access.

Here, the government's only interest in secrecy appears to be derivative of a business's commercial interest in purported trade-secret information in software whose operation is supposedly well-documented and widely-known. Even a credible trade secret interest, on its own, will likely fail strict scrutiny. *See DVD Copy Control Ass'n v. Bunner Inc.*, 31 Cal. 4th 864, 883 (2003) (explaining that the Supreme Court has "recognized that the First Amendment interests served by the disclosure of purely private information like trade secrets are not as significant as the interests served by the disclosure of information concerning a matter of public importance") (citing *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759 (1985)); *see also Woodford*, 299 F.3d at 880 (explaining that narrow tailoring does not comport with "forc[ing the public] to rely on the same prison officials who are responsible for administering the execution to disclose and provide information about any difficulties with that procedure").

The complete denial of source code used on the public's behalf to seek to convict a criminal defendant would surely be an "exaggerated response" to private-interest concerns. *Woodford*, 299 F.3d at 880. In the context of the First Amendment analysis, private concerns like supposed trade secrets should give way to the bedrock constitutional rights held by a criminal defendant and the public.

It is particularly equitable to require the disclosure of trade secrets relating to forensic technology. Private entities developing forensic tools should foresee that absolute secrecy of proprietary information will conflict with the strong public interest in the judicial system's transparency and reliability, as well as defendants' rights of confrontation and due process. This

is especially clear where the product is explicitly marketed for use in the administration of criminal justice, as is the case for TrueAllele.[26]

Moreover, forensic technology businesses have alternative means of establishing competitive advantages besides claiming trade secrecy, including utilizing other legal regimes to challenge commercial infringement of copyright or patent rights in their technology or generating positive publicity through independent testing of non-secret software. A company's strategic choice of one business model over another cannot overcome either the public interest in transparent and fair justice, or a defendant's due process rights.

Thus, even if there were a compelling reason to avoid full disclosure, which there is not, the court should seek to avoid the potential "devastating effect" of overly broad protective orders that prevent expert findings in one case from spreading to others, where they would be equally relevant and useful. Wexler, *supra*, at 1412–13.

CONCLUSION

For the foregoing reasons, *amici* respectfully recommend this Court deny the government's motion to quash.

Dated: July 24, 2020

Respectfully submitted,

/s/ *Hannah Zhao*
Hannah Zhao (NY 5468673)
(*pro hac vice*)
Kit Walsh (CA 303598)
(*pro hac vice* application pending)
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 436-9993
Email: zhao@eff.org; kit@eff.org

[26] *See What can Cybergenetics do for you?* Cybergenetics, https://www.cybgen.com/services/

Sara J. Rose (PA 204936)
ACLU of Pennsylvania
P.O. Box 23058
Pittsburgh, PA 15222
Tel.: (412) 681-7736
Email: srose@aclupa.org